Hardening and Hacking vSphere and Private Cloud RAZR's Edge

Everything you need to know about vSphere Security

Course Details

Level: 2

Course Title: VPCSEC-5

Duration: 5 Days

Language: English

Delivery Methods

Instructor Led Training
Instructor Led Online Training

Participants: Security Administrators and Engineers, Pen Testers, Virtualization/Cloud Administrators, and Engineers, System Engineers and Administrators

Technology: vCloud Suite 5.5, vSphere 5.5, vCAC 5.5, vCOps 5.5, vCloud Networking and Security 5.5. All previous 5.x versions discussed.

Certifications and Exams

RAZR Certified Virtualization Security Engineer (R|CVSE)
RAZR Certified Virtualization Security Specialist-V (R|CVSS-V)

Prerequisites

Two Years IT Security Experience, Network+ Certification or Equivalent Knowledge, Two Years' Experience with Microsoft or Linux Servers, Basic Virtualization/Cloud Knowledge

Introduction

We are well aware that virtualization has been widely implemented, however, there are questions regarding adequate considerations for security threats, known or perceived. It appears that many organizations rest on superior security at the physical layer for a secure virtual layer. This is due in part to an organization that is not aware of the risks associated specifically with the virtual layer or individuals that lack the knowledge to implement adequate security measures. This course changes everything.

This course covers all known and many perceived risks, demonstrates how to hack some of those risks and covers the best hardening practices known today. It covers many technologies related to the VMware vCloud Suite so that you know what you can and cannot do with the software as well as what needs to be added to your security posture to ensure a secure private cloud!

Why Attend this Course

- Learn the latest technologies used to secure the vSphere and Private Cloud Infrastructure.
- The risks to a virtual datacenter are higher than most organizations realize, be prepared to mitigate those risks.
- Become a leader in the industry by staying on top of the security issues related to the private cloud.
- We cover the best third party solutions related to virtualization and the private cloud.
- This course will teach you how to test some of these known risks.
- Our team of developers have worked in the security field for many years, they pioneered today's designs for a secure virtual infrastructure and wrote the first course on virtual security, they have tried and true best practices throughout this course.
- Be prepared to pass both exams:
    - RAZR Certified Virtualization Security Engineer (R|CVSE)
    - RAZR Certified Virtualization Security Specialist-V (R|CVSS-V)
- Take the VM's home with you for additional work after class!
- **50% of your time will be hands on!**

Hardening and Hacking vSphere and Private Cloud RAZR's Edge

Everything you need to know about vSphere Security

Student Materials:

Student Workbook – 600+ Pages
Student Lab Guide – 300+ Pages
Student Lab VM's (60 Day Usage)

Course Objectives

You will learn:

- Latest technologies in securing a virtual and private cloud infrastructure
- Foundational concepts in virtualization security
- How to Securely designing your infrastructure for today and tomorrow
- The best third party security solutions on the market today
- The latest risks known to the vSphere product
- How to audit vSphere
- Details on the vCloud Networking and Security Product
- Implementation of Endpoint security
- The best built in security controls for the vSphere products
- Why virtualization can make your infrastructure more secure
- How to Harden the entire infrastructure, not just a few items

Outline

Chapter 1 – Course Introduction

Chapter 2 – Virtualization and Cloud Overview

1. Overview of Virtualization
2. Overview of Cloud Technologies
3. Design
    a. Functional Requirements
    b. Security Implications
    c. Examples

Chapter 3 – Developing a vSphere Private Cloud Security Posture

1. CIA Triad
2. Threat Modeling
3. Emerging Threats
    a. External Threats
    b. Internal Threats
4. Seven Step Approach to a Desired Security Posture
5. Control Architecture

Chapter 4 – vSphere Native Controls

1. ESXi Secure Architecture and know risks
    a. vCPU
    b. vMemory
2. Virtual Machines Secure Architecture and known risks
    a. Virtual Machine Hardware
    b. Virtual Machine Files
    c. vCenter Features
        i. Clones
        ii. Templates
        iii. Linked Clones
        iv. Snapshots
        v. Logging
3. Host and Cluster Native Controls and known risks
    a. Roles and Permissions
    b. Resource Pools
    c. VMKernel Preventative Controls
    d. vSphere 5.x Preventative Controls
    e. ESXi File Systems Structure
    f. Logging

Appendix – Additional Products only covered in extended hour's delivery (Bootcamp Format)

1. vCloud Native Controls
    a. How vCloud functions with vSphere
    b. Roles and Permissions
    c. Tenant and Landlord Controls
    d. vNetwork Controls
    e. vStorage Controls
    f. vApp Controls
2. Compliance and vCenter Configuration Manager
    a. Overview of Compliance
    b. How Configuration Manager Helps
    c. Key components
    d. Free Compliance Checking Tools
3. Additional vCloud Networking Deep Dive
    a. Edge
    b. VXLAN
    c. Data Security